安全小课堂第九十三期【Alice的白帽子之路】

京东安全应急响应中心 5月2日

JSRC从2013年成立到现在，白帽师傅和我们共同经历了5个春秋，在这些不长不短的日子里，JSRC积累了一箩筐的白帽子成长故事。这些白帽子故事，有些感人，有些励志，也有些坎坷。看上去，白帽子们的日子很美好，每个重要节日都能收到JSRC送的节日礼品，能从JSRC挖掘漏洞换取苹果三件套，一年能从JSRC兑换多达十几万的礼品卡。

但JSRC知道，每一个白帽子走到今天都不容易，知道他们的付出，知道他们的心酸，知道他们一直在努力学习。

JSRC **安全小课堂第九十三期**，邀请到**Alice**师傅为大家分享自己的白帽子之路。同时感谢白帽子们的精彩讨论。

你的成长史-如何成为一个佛系白帽子?

京安小妹

Alice：

各位大表锅好，我在JSRC的ID是Alice。这周被小妹邀请参加小课堂~，很荣幸哈哈~感谢JSRC，感谢小妹。本期也是比较逗比的方式来跟进行。我的日常就是个比较逗比的人。下面讲讲我的一个入坑经历吧。我是在16年初才入的坑。那是一个夜黑风高的夜晚，我照旧在宿舍刷夜打联盟。随着一声雷声响起，屏幕变成黑白。我脑子突然一震，意识到我不能再这么堕落下去。于是乎退出游戏，开始再网上瞎搜。然后“黑客”这个关键词又出现再我脑子里。于是乎。就开始各种搜索。开始逛各种论坛。也知道了乌云。从那天之后，开始各种搜教程。各种看，各种学，各种问。就这样，入了坑。当年16岁的我。也算是比较庆幸，遇到了我们团队老大，被带着入坑，少走了很多弯路。以及各位给我提供帮助的小伙伴们。谢谢大家。所以每当有人问我如何入门时，感触就特别深，哈哈哈，就仿佛看见了当年的自己。也会给他们一些建议。

那么为什么要做一个佛系白帽呢？

是这样的，从我入坑到现在。一路走来。经常会看到很多白帽子跟漏洞平台审核“撕逼”的情况。而很多情况下，都无法调解。我想，可能很多白帽子是没“上过班”的情况。不了解平台内部的一些情况。往往出发点还是以个人为中心。往往忽视了平台的看法。但也有特殊性。这里就不多说了。所以我觉得还是看开点，当一个佛系白帽比较好。挖到洞是福气，挖不到那是命。

讲师

如何做到只蹭蹭不进去呢？真的忍得住吗？

京安小妹

Alice：

哎呀，说起这个就有点害羞~~都怪小妹，起这么污的议题，带坏我了。哈哈哈，是可以做到的。首先说说为什么这样吧。因为一些忍不住的人，往往就造成了无法改变的后果。比如堕胎。呸呸呸。说哪去了。。。我依然记得当初逛乌云的时候，很多白帽子就经常脱裤。然后把密码解密。再去撞库。再进后台。然后进内网测。这样分会给的高。然后在报告最下面写上。数据已删。但到底删没删。谁也不知道。所以，再刚入门时，我们团队内部就有规定，不允许挖上传漏洞，不允许往人家服务器写东西，不允许拿Shell。至始至终，我就拿过一个Shell，当时主要是被这个厂商气死了。所以老大也给了我一次例外。

就好像这次JD出国游的活动吧。我就找了好几个后台。就直接提交了。我就蹭了一下。真的没有进去噢~。其实主要还是不想给自己惹那么多麻烦吧。因为无论是积分还是排名，对我来说都不是特别重要，重要的是你认可我这个洞，并且修了。这就够了。所以不管是挖到一个后台地址对外开放，还是进后台以后再拿shell。对我来说是没啥区别的。要的东西不一样，可能这就是我比较奇葩的原因吧。

讲师

手动信息收集的好处

京安小妹

Alice：

那么，信息收集现在大部分用的都是自动化工具或者半自动化的工具。因为它可以帮助我们节省很多力气。提高挖洞的效率。节省时间。就比如我们团队弄的一个shell脚本一键子域名收集工具。http://www.farmsec.cn/?p=321 很简单就可以完成一键收集子域名。但大多数自动化工具都会有一个问题。那就是是工具在跑。而你却不了解厂商业务。所以再厂商相对于比较小的时候。我更倾向于去手工搜索。这样做最大的好处就是能更加了解厂商的业务。厂商的架构。运营模式等。自动化工具有时候也会“骗人”。我之前遇到过工具访问的时候是显示404的网站，但手工测试的时候发现是误报。于是尝试跑目录。最后挖到一个未授权访问的漏洞。

shodan搜索/与信息收集的小技巧

京安小妹

Alice：

有的有的，比如shodan的搜索，百度云的搜索，Github，码云，乌云镜像，还有一些威胁情报平台等。就好比使用shodan搜索的时候，可以尝试通过搜索尝试的icon。然后发现尝试的业务。很多网站都有属于自己的icon。又或者说，许多网站会有属于自己的Server名字，贴上自己的专属标签。搜索的时候也可以搜索Server：JDWS。只要是shodan支持的，都可以搜索。通过搜索这些特别点。可以寻找更多属于厂商的业务。

讲师

测试中应该注意什么事

京安小妹

Alice：

多的，还是按住自己那颗躁动的心吧。每次我挖洞的时候都会提醒自己耐心点，别着急。总会挖到的。然后过一段时间就挖到了。心情就好了哈哈哈。其次是如果进后台的情况下。一定要把Burp或者其他的爬虫给关闭掉。不然可能会捅娄子。比如重置后台等。再然后就是进入一些电商、金融的时候。可以忍得住诱惑。。。做一个安静的佛系白帽。我最多是见过钱的一个平台。转账交易金额已经过亿了。看来我还是很能忍的哈哈哈。共勉~ （再这里，应该一首归途送给大家。手动艾特遗忘表哥。广告费了解一下）

：

讲师

想对JSRC说的话

京安小妹

Alice：

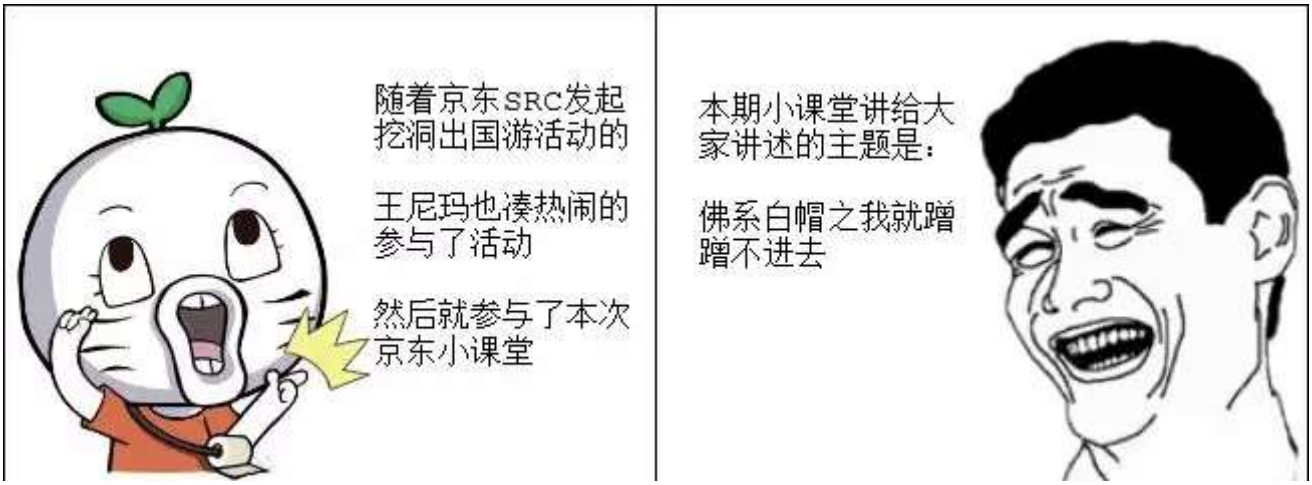
我觉得JSRC是一个很好的SRC平台。群里的老哥个个都是人才，说话又好听，又会斗图。我超喜欢这里的。也认识了很多大表锅~~希望以后可以跟各位大表锅多多学习。其实我就想说一句。小妹，求求你换个头像吧。最后，分享一些自己入坑后收集的一些博客给大家。国内外都有，自从乌云没了之后我就经常逛Hackerone了。感觉老外的思路还是很nice的。因为他们看待安全的问题观点跟国内还是稍有不同的。

http://wiki.secbug.net
http://shentoushi.top
https://www.hacker-arise.com/
https://github.com/pandazheng/SecuritySite
https://blog.feedspot.com/cyber_security_blogs
https://packetstormsecurity.com
http://wiki.jeary.org
https://www.securitysift.com/
https://hk.saowen.com/a/6b19deac68db081640e42f3ce3cb675b45bfda00a9e232399f6dfae335581b6c
https://ngailong.wordpress.com/
https://www.arneswinnen.net/
https://www.geekboy.ninja/blog/
https://pentesterlab.com/
https://blog.zsec.uk/
https://mishresec.wordpress.com/
https://linuxhint.com

：

讲师

感谢Alice做的图以生动有趣的形式展示了本期小课堂，点赞👍



Hi Alice，做一个佛系白帽有什么好处吗？

是这样的，从我入坑到现在。经常会看到很多白帽子跟审核"撕逼"

我也会经常找审核大大"撕逼"。但是我跟其他白帽子不一样的是，他们"撕"的是你给我几个金币。而我"撕"的是你对我提的洞是不是认可的。

我"撕"的是情怀~~

那，如何做到只蹭蹭不进去呢？真的忍的住吗？（手动捂脸）

哈哈，是可以做到的。我记得当年乌云还再的时候，很多白帽子就经常脱裤。然后拿到账号密码。再去撞库。然后在底下留言数据已删。然而到底删没删。谁也不知道。

像这次JD的活动。我找了好几个后台。就直接提交了。没有再进去。主要，还是不想给自己惹麻烦吧。

下一个问题，手工信息收集的好处是什么？

信息收集现在用的基本上都是自动化或者半自动化的工具，手工信息收集分很多部分。最大的好处就是，能更加了解厂商的业务、运营模式。

自动化工具有时候会"骗人"。我之前遇到工具报404的网站，但手工测的时候发现是误报。最后尝试跑目录。挖到一个未授权访问漏洞。

那你有什么信息收集的小技巧吗？

有的，有的~~
比如shodan的搜索小技巧
百度云的搜索
GitHub的搜索
还有一些威胁情报等

请看下图~

很多网站都会有属于自己的icon。使用shodan搜索时，可以通过搜索该icon。然后找到厂商的业务~~

许多网站会有属于自己的Server 贴上自己的专属标签~~~

可以通过搜索这些Server，寻找更多属于厂商的IP地址，基本都是准的

在进行渗透测试时，应该注意什么呢？

注意事项其实挺多的。更多的还是按住自己那颗躁动的心吧。我每次挖洞都会提醒自己耐心点，别着急总会挖到的。

然后就是如果进了后台一定要吧burp的爬虫给关了~~

这个很重要~~

最后一个问题，你有什么话想对JSRC说呢？

我觉得JSRC是一个很好的SRC平台。群里的老哥个个都是人才，说话又好听，又会斗图。我超喜欢这里的。也认识了很多大佬~~

其实我就想说一句。

本期JSRC 安全小课堂到此结束。更多内容请期待下期安全小课堂。如果还有你希望出现在安全小课堂内容暂时未出现，也欢迎留言告诉我们。

安全小课堂的往期内容开通了自助查询，点击菜单栏进入“安全小课堂”即可浏览。

简历请发送：cv-security@jd.com

微信公众号：jsrc_team

新浪官方微博：京东安全应急响应中心